May 29, 2003
File Name: levels052903.doc

Conformance Levels for Government Smart Card
A Draft Proposal

NOTE: (This is a strawman paper to serve as a basis for discussion)

The Government Smart Card Interoperability Specification (GSC-IS) Version 2.1 defines the interoperability requirements that all systems purchased under the General Services Administration Common Access Smart ID card contract must meet. Products available under the GSA contract will be subject to a certification process using the GSC-IS Conformance Test Program.

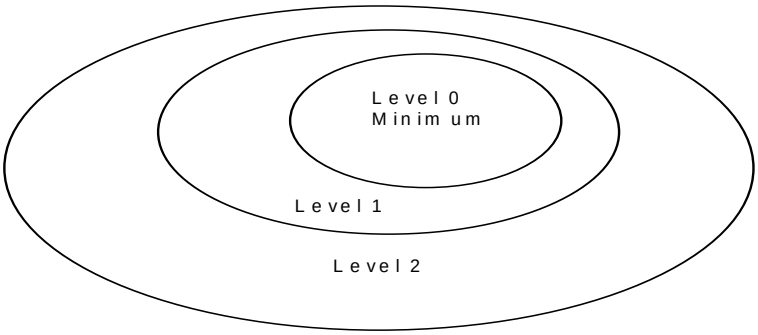
The GSC-IS defines an SPM that provides two application interfaces and considerable functionality. An implementation of the entire GSC-IS system could be large. However, not all functionality may be required for every application. In the design of the GSC-IS conformance criteria, we need to organize the functionality of the specification into increasing supersets, or levels, beginning with a minimal set that is applicable to all implementations, and ending with the set consisting of the entire functionality specified in the GSC-IS.

The purpose of this draft paper is to develop these levels of functionality. The suggested levels may then be used as the basis for certification levels to be used in connection with the conformance testing process. Thus, products may be certified for a particular level of conformance.

Levels and Profiles of Conformance

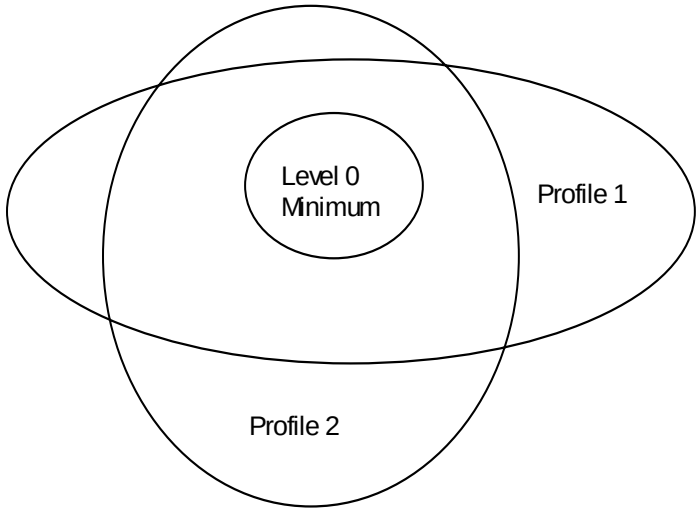
There is a requirement that the conformance criteria for the GSC-IS partition the specified functionality into levels and/or profiles.

Levels of conformance reflect a partitioning into increasing supersets of functionality, beginning with a minimal set that is applicable to all implementations, and ending with the set consisting of the entire functionality specified in the GSC-IS.



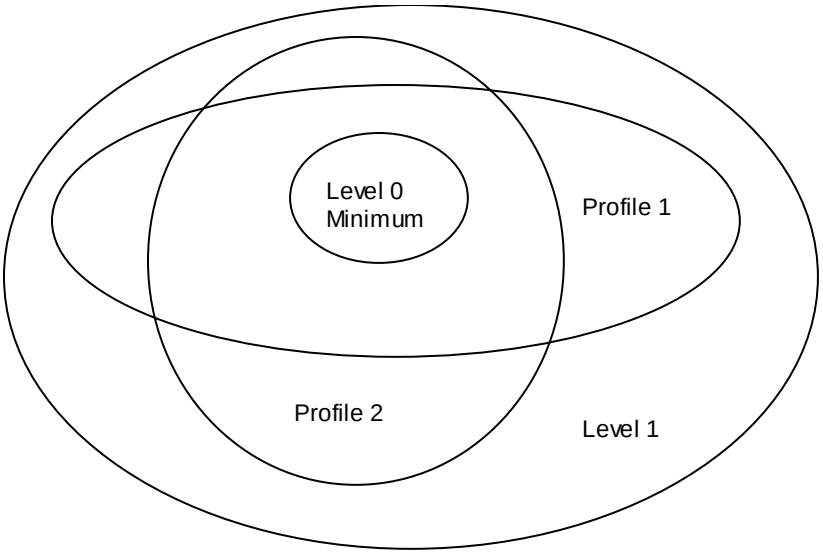
Example of a Levels structure

Profiles constitute a less rigidly constructed collection of sets of functionality. Each profile must contain the minimal set, but otherwise can partially intersect, or be disjoint from, other profiles. Profiles may be designed for particular applications or user communities.



Example of Profile Structure

It is possible that a profile structure can be combined with a level structure:



Example of a combined Levels and Profiles structure

Level 0

Level 0 is the minimum level of the GSC-IS, containing the functionality that all products must implement. An application implementing only Level 0 might be a physical access badge with no authentication. The only identity authentication is for the bearer to possess a conformant card. The SPM implements simple BSI utility commands, and also the gscBsiPassthru command to enable the sending and receiving of APDUs. For card edge interfaces, only the file system APDUs as appeared in Table 5-1 of GSC-IS v2.1 are considered here.

Level 0 BSI:
A conformant SPM must support:

- gscBsiUtilConnect
- gscBsiUtilDisconnect
- gscBsiUtilGetVersion
- gscBsiUtilGetCardProperties
- gscBsiUtilGetCardStatus
- gscBsiUtilGetExtendedErrorText
- gscBsiGetReaderList
- gscBsiUtilPassthru

Level 0 CEI
A conformant SPM must support:

- Select Master File
- Select File
- Select EF under Selected DF

Read Binary

Level 0 Cards:

A conformant card must implement either the GSC or CAC data model.

Level 1

Level 1 provides physical access with authentication. It includes all the functionality at Level 0, and also allows information from card containers to be read, but not written to or updated.

Level 1 BSI:

A conformant SPM must support Level 0 plus the generic container functions:

gscBsiGcGetContainerProperties
gscBsiGcReadTagList
gscBsiGcReadValue

Level 1 CEI:

A conformant SPM must support Level 0 plus:

Select DF
Get Response

Level 1 Cards:

Must support Level 0.

Level 2

Level 2 provides the functionality of an Electronic ID token by considering the environment of the smart card and the smart card reader connected to a PC system. The PC system and the smart card must have mutual authenticating authority (i.e., be capable of doing internal and external authentication) and they must be able to share a secret (i.e., use PINs and challenges). Level 2 supports the ACR rules as specified in Chapter 3 of the GSC-IS. This level does not support PKI.

Level 2 BSI:

A conformant SPM must support Level 1 plus:

gscBsiUtilAcquireContext
gscBsiUtilReleaseContext
gscBsiGcDataCreate
gscBsiGcDataDelete
gscBsiGcUpdateValue
gscBsiGetChallenge
gscBsiSkiInternalAuthenticate
gscBsiGetCryptoProperties

Level 2 CEI:
A conformant SPM must support Level 1 plus:

- Update Binary
- External Authenticate
- Get Challenge
- Internal Authenticate
- Verify

Note: The question comes up at this point about file system vs virtual machine cards. Do we need to list them separately for levels 2, 3

Level 2 Cards:
Must support Level 1.

Level 3

Level 3 supports PKI. The SPM must be able to perform a private key computation on the message digest using the private key associated with the specified AID.

Level 3 BSI:
A conformant SPM must support the entire BSI, i.e., Level 2 plus:

- gscBsiPkiCompute
- gscBsiPkiGetCertificate

Level 3 CEI:
A conformant SPM must support the entire CEI, i.e., Level 2 plus:

- Manage Security Environment
- Perform Security Operation

Level 3 Cards:
Must support Level 2.